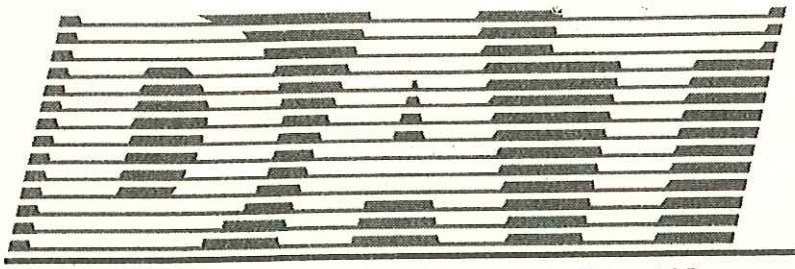
Hacia un marco europeo de la firmas digitales y la encriptation

Vinje, Thomas; Julia, Rosa

Published in:
D.A.T.

Publication date:
1998

Document Version
le PDF de l'éditeur



DERECHO DE LA ALTA TECNOLOGIA

Una publicación de Estudio Millé, Buenos Aires, Argentina.

AÑO X - Nº 115 - MARZO 1998

En este número:

Hacia un marco europeo de las firmas digitales y la encriptación

por Rosa Julià-Barceló y Thomas Vinje

El crecimiento de la comunicación electrónica depende de la seguridad y confidencialidad que pueda darse a los mensajes. La necesidad de confidencialidad y seguridad existe en una gran variedad de comunicaciones electrónicas, incluyendo, por ejemplo, contratos electrónicos (tanto interempresarios como entre la empresa y el consumidor) declaraciones de impuestos electrónicos e historias médicas electrónicas. Tal como se describe luego, las principales herramientas tecnológicas para asegurar la confidencialidad y seguridad de las comunicaciones electrónicas son métodos para la firma digital y la encriptación.

El 8 de octubre de 1997, la Comisión Europea dio un paso adelante estableciendo un marco europeo para las firmas digitales y la encriptación, al emitir una comunicación titulada "Asegurando seguridad y confianza en las comunicaciones electrónicas: Hacia un marco europeo para las firmas digitales y la encriptación". La Comunicación está dividida en tres secciones. La primera sección trata de la elaboración de un marco reglamentario para las entidades que emiten los certificados estableciendo las bases para las firmas digitales (las así llamadas autoridades de certificación) y sobre el reconocimiento legal de las firmas digitales. La segunda sección trata de las medidas de encriptación, incluyendo las medidas de control de exportaciones y los requisitos para su aplicación. Finalmente la Comunicación discute las bases legales para una iniciativa de la Comisión en esas áreas y el alcance y agenda de tal iniciativa.

Luego de efectuar una introducción a la tecnología del caso, este artículo proporcionará una breve descripción y análisis de los principales tópicos discutidos por la Comunicación, enfocándose particularmente en firmas digitales y autoridades de certificación.

1. Una introducción a la Tecnología

Tanto las firmas digitales como la encriptación se basan en las tecnologías de la encriptación. Realmente, una firma digital es esencialmente un mensaje encriptado, que acompañan un documento electrónico. No obstante, como se describe más abajo, las firmas digitales y la encriptación tienen diferentes funciones y usualmente se basan en diferentes tipos de técnicas criptográficas.

Encriptación

Tal como se usa en la Comunicación, "encriptación" es el término empleado para describir los sistemas de clave simétrica usados para mantener la confidencialidad de las comunicaciones electrónicas. Mediante el intercambio de mensajes encriptados usando criptosistemas simétricos (como se describen más abajo), los interlocutores en una comunicación buscan asegurarse de que ellos (y solamente

ellos) serán capaces de leer el contenido de los mensajes.

En los sistemas de claves simétricas, tanto el emisor como el receptor usan la misma clave para encriptar y desencriptar los mensajes: el emisor encripta un mensaje con la clave simétrica y lo envía al receptor, el cual posee la mismo clave y la usará para desencriptar el mensaje (esto es: para volverlo a poner en texto claro). Para que las comunicaciones permanezcan confidenciales, la clave debe permanecer secreta. Esto significa que los partes deben tener una vía segura para intercambiar sus claves. Como la Comunicación hace notar, esto es complicado en un ambiente abierto, donde muchos participantes no se conocen los unos de los otros.

Aún cuando la Comunicación usa el término encriptación para describir únicamente sistemas que usan claves simétricas, es también posible, tal como se describe luego, obtener confidencialidad en las comunicaciones usando criptografía asimétrica.

Tecnología de firma digital

En tanto que la encriptación tal es el término que se emplea en la Comunicación se usa para lograr confidencialidad, la tecnología de la firma digital se utiliza para alcanzar integridad y autenticidad de los datos, esto es, seguridad de las comunicaciones electrónicas. Por medio del uso de la tecnología de firma digital, el receptor de una comunicación electrónica puede estar seguro de que el emisor de la comunicación es realmente quien dice ser (esto es denominado frecuentemente *función de autenticación de la firma digital*). Las partes comunicantes pueden también asegurarse que la comunicación recibida es la que se remitió realmente (esto es frecuentemente aludido como *función de integridad de las firmas digitales*).

La tecnología de la firma digital se basa en sistemas de encriptación asimétricos, en los cuales se usan claves diferentes para la encriptación y para la desencriptación. Con sistemas asimétricos cada parte recibe dos diferentes claves. Una clave se usa para transformar ciertos datos en una forma aparentemente ininteligible. Estos datos se agregan a un documento electrónico y efectivamente constituyen la firma digital misma. Otra clave se usa para verificar una firma digital devolviendo los datos a su forma inteligible original. En otras palabras, el emisor de una comunicación electrónica la firma digitalmente añadiendo a ella ciertos datos encriptados usando una clave (en una forma muy similar a la de un autor de un documento tradicional en papel que lo firma añadiendo su firma manuscrita al mismo). El receptor del documento electrónico se asegura de la validez de la firma digital mediante la desencriptación de los datos usando otra clave.

La clave usada para crear la firma digital - la clave "de firma" - se llama la *clave privada*, porque está disponible solamente para el firmante. Salvo que esa clave haya sido robada o penetrada de alguna otra forma nadie puede tener acceso a esa clave privada, y en consecuencia nadie podría firmar un mensaje de esta manera.

El segundo elemento del juego "de claves asimétricas" que sirve para verificar la firma se llama *clave pública* porque usualmente se pone a disposición del público en general, por ejemplo por medio de un directorio de claves públicas. Cuando se aplica a firmas digitales creadas por los titulares de claves privadas desencriptará esa firma y solamente esa firma. En consecuencia, la clave pública no reconocerá la firma digital de ninguna otra persona.

En razón de que una clave pública en particular puede verificar solamente firmas digitales creadas usando la clave privada de su propietario, y en razón de que (salvo que la clave haya sido penetrada) el emisor de un mensaje es el único posesor de la clave privada, el recipiente de un mensaje que usando la clave pública del emisor, verifica exitosamente la firma digital que lo acompaña puede confiar que el mensaje es auténtico, esto es, que fue enviado por la persona que se presenta como emisor. Más aún, luego de aplicar la clave pública al mensaje encriptado, el receptor puede comparar el texto resultante con el texto en claro incluido en el mensaje. Si resultan ser el mismo, el receptor puede también confiar sobre la integridad del mensaje (esto es, que el mensaje no fue alterado durante el mensaje).

En muchas técnicas de claves públicas, un algoritmo de una sola dirección (un así llamado *algoritmo hash*) se aplica a un mensaje electrónico para producir una versión condensada del mismo. Esta versión condensada del mensaje (el sumario del mensaje) es entonces firmado (encriptado) con la clave privada del emisor. En efecto, este sumario del mensaje encriptado es en sí mismo la firma digital.

Dado que el método *hashing* es una función de una sola dirección, el sumario del mensaje no puede ser dado vuelta por el receptor para obtener el mensaje completo. En consecuencia, el sumario del mensaje encriptado (la firma digital) se acompaña por el texto completo del mensaje en forma encriptada. Luego de recibirse, el receptor procesa el texto del mensaje no encriptado con el mismo algoritmo *hash* que se usó para crear el sumario del mensaje, y compara el sumario de mensaje resultante con el original que el emisor le envió junto con el mensaje (el cual, naturalmente el receptor ha desencriptado usando la clave pública del emisor). Si el mensaje no encriptado fue alterado de alguna manera durante el tránsito, los dos sumarios serán diferentes y en consecuencia revelarán las alteraciones que hubieran sido introducidas[2].

Con respecto a la autenticidad de un mensaje, los receptores pueden confiar en la identidad del emisor solamente si también confían en que las respectivas claves privadas permanecen en la sola posesión de la persona con la cual ellos creen que están comunicándose, también en que la parte con la que estén comunicándose sea realmente la persona quien afirma ser. Por ello, el sistema de claves debe permitir al receptor de una comunicación electrónica asegurarse que la clave privada no haya sido comprometida. Por ejemplo, una farmacia debe estar en condiciones de controlar fácilmente si la clave privada de un médico ha sido robada o comprometida de alguna otra forma antes de despachar el pedido de un medicamento en una receta emitida por este médico. Más aún, es frecuentemente importante para el funcionamiento del sistema permitir al receptor de una comunicación electrónica asegurarse no solamente de que la parte con la cual el receptor se está comunicando es realmente la que se piensa que es, sino también que la misma tiene ciertas características. Por ejemplo, una farmacia puede necesitar establecer que el titular de una particular clave es realmente un médico, antes de aceptar su firma digital en una receta electrónica. Como se describe más abajo, ambos objetivos pueden alcanzarse por medio de las actividades de las autoridades de certificación.

Es una práctica común incluir la clave pública junto con una comunicación electrónica. No obstante, no proporciona suficiente confianza sobre la integridad de la clave privada. Aún cuando el receptor puede usar una clave pública que fue acompañada a la publicación para desencriptar la firma, la única manera de lograr la real confianza en la firma digital es recuperar la clave pública de una base de datos confiable y desencriptar esa firma digital usando esa clave pública. El hecho de que una clave pública se incluya junto con una comunicación y de que esa clave pueda ser usada para desencriptar esa firma digital no significa que la clave privada permanezca en la sola posesión del correcto titular de la clave.

Tal como se describe más abajo, esto pone en relieve, una de las más importantes funciones de las autoridades de certificación, o sea el establecimiento y mantenimiento de bases de datos de claves. Al emitir certificados a tenedores de claves y al crear y actualizar bases de datos de claves, las autoridades de certificación juegan un rol esencial para establecer un sistema confiable en el cual los receptores de mensajes puedan verificar la integridad de las claves privadas y las características del titular de tales claves.

En consecuencia, la firma digital llena las mismas funciones básicas de autenticidad e integridad de la firma manual: Realmente, con un sistema de clave pública y clave privada bien estructurado y administrado que usa algoritmos seguros y claves de suficiente extensión es virtualmente imposible penetrar una firma digital, por lo que una firma digital es mucho más confiable que una firma manual[3]. Un sistema de comercio basado en documentos electrónicos y firmas digitales tiene en consecuencia, el potencial para proveer más seguridad que nunca antes.

Como ya se ha hecho notar, la criptografía asimétrica puede usarse no solamente para asegurar autenticidad e integridad mediante la tecnología de la firma digital, sino también confidencialidad. Realmente las comunicaciones electrónicas acompañadas por firmas digitales se encriptan frecuentemente usando las claves públicas de los receptores. En consecuencia, el receptor y solamente el receptor- puede usar su clave privada para desencriptar las comunicaciones.

El rol de las autoridades de certificación

Como se hará notar, la confiabilidad de las firmas digitales y en consecuencia su valor en el comercio electrónico , reposa sobre la *confiabilidad de las claves*. En un ambiente abierto, la requerida confiabilidad de las claves puede alcanzarse principalmente mediante el establecimiento de un régimen legal que reglamente las autoridades de certificación dependientes que proveerán: 1) la seguridad necesaria acerca de la identidad, mediante la emisión de certificados que liguen claves públicas con la identidad de sus dueños y 2) la confianza requerida acerca de que estas claves no han sido comprometidas, mediante el establecimiento de una base de datos confiable que mantenga una lista actualizada de claves varias [4].

En orden a dar confianza a las partes que se comunican acerca de la identidad y características de un titular de claves, la autoridad de claves debe obtener y verificar cierta información para el certificado. Por ejemplo, un médico que solicite un certificado debe proporcionar una demostración adecuada de su identidad personal y de su licencia como médico. Luego de haber obtenido y verificado tal información, la autoridad de certificación crea un documento conteniendo, entre otras cosas, la clave pública de las partes[5], la identidad del titular de la clave, un número de serie y la identidad de la autoridad certificante. Entonces se aplica una función *hash* a esta información y la misma se firma por la autoridad certificante con su clave privada. Esta firma es entonces añadida a la misma información en forma no encriptada en orden a integrar el certificado. Entonces, el certificado tiene dos partes: la parte no encriptada: la información en texto llano y la firma digital de la autoridad certificante.

Estos certificados permiten a las partes que se comunican, lograr confianza acerca de la identidad y estatus de las partes con las cuales ellos quieren comunicarse de la siguiente forma: cuando la parte A entra en una transacción con la parte B enviando a la parte B un mensaje firmado digitalmente por la parte A, ésta envía también junto con el mensaje el certificado emitido por la autoridad certificante. Por cuanto el certificado contiene la clave pública de la

librados por las autoridades que cumplan con este régimen, debe considerarse laudable. Además, la Comunicación parece sugerir el establecimiento de un régimen flexible que daría lugar para experimentación en esta nueva área, evitando la creación de pesadas obligaciones burocráticas.

↳ El sistema legal que reglamentará el establecimiento y operación de las autoridades de certificación ¿debería basarse en un sistema de licencias, en uno que no se fundara en ella o en los dos regímenes?

Una de las cuestiones clave que deben considerarse en conexión con la creación de un régimen armonizado para el establecimiento y operación de autoridades de certificación, es si las autoridades de certificación deberían ser licenciados por los gobiernos y si los Estados Miembros que requirieran licencias deberían aceptar los certificados emitidos por autoridades no licenciadas en un Estado Miembro donde no exista obligación de obtener licencias. Tal como la Comunicación indica, algunos Estados Miembros están actualmente en el proceso de introducir esquemas voluntarios para el establecimiento y operación de autoridades de certificación, en tanto que otros contemplan esquemas de licencias obligatorias como elemento esencial para desarrollar confianza en las autoridades de certificacción y en las firmas digitales en las autoridades de certificación y en las firmas digitales[7].

La Comunicación acepta que los regímenes de licencia podrían ser apropiados. No obstante, acepta también la posibilidad de enfoques sin licencia. Realmente, dice "el licenciamiento es solamente uno de los métodos posibles para aumentar la confianza, que los Estados Miembros pueden aplicar para promover el uso de firmas digitales comúnmente válidas. Organizaciones públicas o privadas no licenciadas, pero altamente vigiladas pueden también ser consideradas como autoridades de certificación confiables". De todas formas, la Comunicación concluye que el régimen de la Unión Europea reglamentando las autoridades de certificación debería permitir la "coexistencia de autoridades de certificación licenciados y no licenciadas". No es claro precisamente lo que implicaría esta coexistencia, pero pareciera que un Estado Miembro que adoptara un sistema de licenciamiento debería aceptar certificados emitidos por autoridades no licenciadas, activas en Estados Miembros que no tuvieran sistemas de licencia. No obstante, las autoridades de todos los Estados Miembros deberían cumplir con todos los criterios mínimos que gobernaran el establecimiento y operación de las autoridades de certificación, impuesto por la legislación de la Unión Europea.

El enfoque de "coexistencia" de la Comunicación parecería ser razonable. Dada la inmadurez de esta área de negocios, la flexibilidad resulta elemento necesario para la experimentación. Por ejemplo, sería apropiado limitar las obligaciones de licencia solamente a aquellas autoridades de certificación que proveyeran servicios al público (como fue sugerido por el Reino Unido) y exceptuar a los grupos cerrados de cualquier requerimiento de licencia. El objetivo fundamental debería ser establecer un balance entre imponer suficientes obligaciones legales en el establecimiento y operación de las autoridades de certificación como para generar confianza en el uso de tecnología de firma digital, al tiempo que dejar un margen de libertad para que las tecnologías y las prácticas de negocios se desarrollen.

↳ ¿Qué régimen de responsabilidad debería gobernar las actividades de las autoridades de certificación?

La Comunicación dice, correctamente, que tener "reglas claras de responsabilidad contribuiría a la aceptación de los servicios de las autoridades de certificación".

No obstante, la Comunicación no define claramente el estándar que prevé para la responsabilidad. Al referirse a temas acerca de la responsabilidad, uno debería distinguir entre los siguientes actores: 1) el titular del certificado; 2) la autoridad de certificación y 3) la tercera parte que recibe el certificado y confía en él.

Con respecto a la potencial responsabilidad de la autoridad de certificación respecto del titular del certificado, con quienes presumiblemente tienen una relación contractual, la Comunicación parece indicar que la responsabilidad estándar de la autoridad de certificación dependerá de los términos del contrato. La Comunicación avanza un poco más para indicar que un "catálogo de requisitos" podría formar la base de las obligaciones contractuales, indicando tanto responsabilidades máximas como mínimas para la autoridad de certificación. No obstante, la Comunicación no indica cuáles requerimientos podría contener este "catálogo", ni tampoco si tal catálogo tendría valor de obligación legal, ni tampoco si el régimen legal que gobernara a las autoridades de certificación debería prohibir la exclusión de responsabilidad en ciertas circunstancias, quizás como una materia de protección a los consumidores. Por ejemplo, ¿una autoridad que omitiera publicar la revocación de un certificado luego de haber recibido una apropiada notificación por el titular acerca del robo de ese certificado debería estar en condiciones de excluir responsabilidad por los daños incurridos por un titular cuando el mismo fuera usado por un delincuente?

Con respecto a la responsabilidad extracontractual, tanto entre la autoridad certificante y las partes que confían en un certificado como el del titular del certificado y dichos terceros, la Comunicación guarda silencio. Hubiera parecido apropiado que cualquier régimen gobernando la

operación de las autoridades de certificación se refiriera este tema y estableciera un régimen de responsabilidad creando un balance apropiado entre los intereses de estos actores.

De acuerdo a las reglas usuales sobre culpabilidad, la persona que sufriera un daño por haber confiado en un certificado tendría la carga de la prueba para demostrar la falta de debido cuidado por parte de las autoridades de certificación. No obstante, dados los aspectos de tecnología muy especializada involucrados en la emisión y mantenimiento de un certificado, esta obligación podría implicar una carga excesivamente difícil de afrontar. De allí que una solución que estableciera una inversión de la carga probatoria podría resultar apropiada. Bajo este enfoque, la autoridad de certificación tendría que probar su falta de negligencia. Quizás, esta inversión de la carga probatoria resultaría igualmente apropiada en el contexto de los casos regidos por contratos entre las autoridades de certificación y los titulares de certificados.

Parece probable que un enfoque de esta naturaleza se adopte por la Comisión de las Naciones Unidas para el Derecho Comercial Internacional (UNCITRAL) en una nueva ley modelo sobre autoridades de certificación que completaría la Ley Modelo sobre Comercio Electrónico[8]. El proyecto de UNCITRAL propone también una presunción de responsabilidad, del tipo de la que se dispone en la Directiva sobre Responsabilidad por Productos Defectuosos, que puede ser rechazada por la autoridad de certificación demostrando que ha llenado ciertos requisitos (por ejemplo, demostrando que actuó con diligencia en averiguar la identidad del tenedor de la clave).

La Ley Alemana sobre Firma Digital no se refiere a reglas especiales acerca de responsabilidad. En consecuencia, los principios comunes en cuestión de responsabilidad se aplicarán en Alemania[9]. Por el contrario, los documentos de consulta pública del Reino Unido sugieren que las autoridades de certificación deberían sujetarse a un régimen de responsabilidad estricta atenuado únicamente por límites de responsabilidad en materia de indemnizaciones[10].

Debe mencionarse un aspecto específico concerniente a la obligación del titular de certificados de mantener el secreto de la clave y notificar inmediatamente a la autoridad de certificación acerca de cualquier compromiso del secreto. Aún cuando algunos autores han criticado la noción de que el titular del certificado deba soportar el riesgo de pérdida por el tiempo que demore en notificar a la autoridad certificante acerca del compromiso de la clave[11], éste parecería ser el único sistema posible de atribución del riesgo. Parecería inapropiado imponer cualquier responsabilidad a la autoridad de certificación hasta que la misma haya recibido tal noticia, aunque resultaría naturalmente útil que las autoridades de certificación educaran a los titulares de certificados acerca de la importancia de mantener la integridad de los certificados y las claves cuidadosamente. Además, medidas tecnológicas, tales como tarjetas inteligentes provistas de implementos biométricos, podrían reducir los riesgos asociados con la pérdida o robo de las claves y certificados.

3. Reconocimiento Legal de las Firmas Digitales

Las firmas digitales no podrán jugar un papel apropiado para facilitar el comercio electrónico hasta que sean reconocidas legalmente. En otras palabras, las firmas digitales deben ser legalmente equivalentes a firmas manuscritas antes de que puedan transformarse en una herramienta efectiva de negocios.

Desafortunadamente, tal como la Comisión lo señala en su Comunicación, las firmas digitales no han recibido apropiado reconocimiento legal. Actualmente el derecho de los Estados Miembros de la Unión Europea impone requerimientos de firmas manuscritas y documentos escritos como condición de validez contractual, ejecutabilidad, valor y admisibilidad probatorios[12]. Tales requerimientos varían de un Estado Miembro de la Unión Europea al otro, tanto en sus términos como en sus propósitos específicos.

En muchos sistemas legales resulta común encontrar un requerimiento de que ciertos contratos o actos administrativos deben realizarse por escrito y hallarse autentificados por firmas manuscritas. Bajo este enfoque, por ejemplo, ciertos contratos resultan inválidos o inejecutables, salvo que se documenten por escrito y estén suscritos por una firma manuscrita, muchas veces por propósitos relacionados con la protección de los consumidores[13]. En otros casos, se atribuye a documentos escritos y firmados mayor valor probatorio que a otros formas de evidencia[14], y no resulta claro si las firmas digitales calificarán para este tratamiento favorable. Más aún, en países donde no se acuerda un estatus privilegiado a la prueba instrumental, los tribunales no siempre están dispuestos a otorgar el mismo valor probatorio a documentos electrónicos acompañados por firmas digitales que el que atribuyen a sus partes convencionales acompañadas por firmas manuscritas.

En tanto las firmas digitales pueden proporcionar por lo menos el mismo grado de confianza acerca de la autenticidad e integridad de un documento que lo que pueden hacer sus contrapartes manuscritas, esta es una situación anacrónica. Tal como la Comunicación hace notar "en orden a alcanzar una aceptación de las firmas digitales tan amplia como resulte posible, los sistemas nacionales pueden necesitar ser adaptados para asegurar que ofrecen el mismo reconocimiento y tratamiento a las firmas digitales que a las firmas convencionales".

A nuestra manera de ver, para facilitar el desarrollo del

comercio electrónico la armonización de la legislación de la Unión Europea deberá establecer el reconocimiento legal de las firmas digitales. La Comunicación parece abrazar esta proposición indicando que la Comisión se propone producir una creciente consciencia acerca de la necesidad de legislar un reconocimiento de la firma digital a nivel comunitario[15]. Al seguir este camino, la Comisión sigue los pasos de diversos comisiones internacionales que han sugerido que se tomen medidas para proporcionar un apropiado reconocimiento legales a nuevos mecanismos de autenticación e integridad (por ejemplo el UNCITRAL, el programa TEDIS, el Consejo de Europa, y el Grupo de Trabajo 4 para la Facilitación del Comercio Internacional de la Comisión de las Naciones Unidas para Europa)[16].

Como señala correctamente la Comunicación, cualquiera de estos regímenes legales deben ser suficientemente flexibles para anticipar desarrollos tecnológicos futuros. Mientras que debería dar a las firmas digitales del momento el mismo reconocimiento que a las firmas convencionales, tendría que adoptar un enfoque tecnológicamente neutral, que pudiera aplicarse también a nuevos medios para proveer autenticación e integridad que aparecieran en el futuro. Realmente, la ley no debería legislar el reconocimiento de una tecnología específica empleada actualmente para la de firma digital, en parte porque esa tecnología podría en algún momento dejar de proveer una seguridad adecuada. El progreso tecnológico podría conducir a una situación en la cual las formas actuales de criptografía de clave pública antes expuestas, no continuarán asegurando integridad y autenticidad (por ejemplo, en razón de que la capacidad de los computadores llegue al punto en que resulte posible descubrir con rapidez una clave privada partiendo de la clave pública o porque ciertos algoritmos de encriptación ya no continúen proveyendo seguridad en razón de que los problemas matemáticos que subyacen hayan sido resueltos). Además, una legislación que se dirigiera específicamente hacia las actuales tecnologías podría desalentar el desarrollo de nuevas tecnologías.

En consecuencia, la Comisión Europea y los Estados Miembros deberían comenzar inmediatamente el proceso de identificar, analizar y catalogar los varios requerimientos legales a consecuencia de los cuales las firmas digitales y los documentos electrónicos resultan desventajosamente discriminados en relación con sus contrapartes tradicionales sobre base papel. Luego, sería necesario emprender la difícil tarea de diseñar un enfoque nuevo y armonizado para estos requerimientos que no esté ya más formulado en la terminología del mundo tradicional de los documentos en papel y que acordarán reconocimiento legal apropiado a las firmas digitales y sus descendientes tecnológicos. Este estándar debería identificar el nivel de autenticidad e integridad requerido para particulares tipo de documento (sean tradicionales o electrónicos) y establecer estándares tecnológicamente neutrales de acuerdo a los cuales cualquier manera de proporcionar la requerida autenticidad e integridad recibiera igual reconocimiento legal[17].

Se presenta en este contexto una importante cuestión concerniente al rol de las autoridades de certificación. Tal como la Comunicación también reconoce, los efectos legales de los documentos firmados con firmas digitales puede ser ligada implícitamente a la confiabilidad de las autoridades de certificación. Realmente, en la medida en que las autoridades de certificación, por ejemplo, aseguren la conexión entre la clave pública y el titular de la clave, las mismas ampliarán el valor y la confiabilidad de las firmas digitales.

No obstante, los nuevos estándares legales (antes mencionados) que gobiernen el nivel de autenticidad e integridad requerido para todo tipo de documentos ¿deberían hallarse dentro de las competencias de una autoridad de certificación? Por ejemplo, ¿deberían las leyes (tal como algunos han sugerido)determinar que el documento electrónico calificará como un "documento escrito" para propósitos probatorios u otros solamente si se encuentra acompañado por una firma digital que haya sido reconocida por una autoridad de certificación que haya llenado ciertos requisitos respecto de su establecimiento y operación? A nuestra forma de ver, una condición tal estaría fuera de lugar, por lo menos en determinado contexto. Por ejemplo, compañías que hagan negocios la una con la otra por vía electrónica podrían muy bien escoger hacerlo intercambiando privadamente sus claves y evitando el gasto y las complicaciones derivados de usar una autoridad de certificación. Parecería inapropiado denegar un auténtico reconocimiento legal a los documentos electrónicos firmados digitalmente en estas circunstancias. Quizás el derecho podría disponer que firmas digitales certificadas por una autoridad de certificación licenciada tuvieran un reconocimiento legal *prima facie*, pero podría autorizar que quienes confiaran en otras firmas digitales probaran su validez demostrando la seguridad y confiabilidad de los sistemas y firmas en cuestión.

Los documentos electrónicos acompañados por firmas digitales certificadas proporcionan un grado de autenticidad e integridad mucho más alto que el de muchos otros documentos convencionales acompañados por firmas manuscritas. De allí que requerir a un documento electrónico que venga acompañado por una firma digital certificada por una autoridad de certificación como condición para que ese documento tenga reconocimiento legal impondría una carga mucho más gravosa a las firmas digitales en comparación con la que se ha impuesto tradicionalmente a los documentos legales por firmas manuscritas. Para muchos -quizás la mayoría- de los documentos electrónicos parecería inapropiado imponer un estándar tan elevado de autenticidad e integridad.

Realmente, requerir a un documento electrónico que esté

acompañado por una firma digital certificada por una autoridad de certificación parecería lo mismo que requerir a toda firma manuscrita que esté certificada por un escribano público. Desde el momento en que no todos los documentos electrónicos necesitan ser notarizados para tenerlos por válidos y ejecutables, ¿por qué se debería requerir a los documentos electrónicos la fijación de una firma digital certificada por una autoridad de certificación en orden a reconocerlos legalmente? Quizás una solución apropiada sería requerir la actuación de una autoridad de certificación solamente en los casos en que en el contexto de un documento convencional se hubiera requerido la intervención de un escribano público y cuando la comunicación se hace por autoridades públicas, tales como la autoridad fiscal o la de seguridad social.

En cualquier caso, un enfoque funcional tecnológicamente neutral debería adoptarse para proporcionar a los tribunales motivos para actuar de una manera flexible y aceptar nuevas formas tecnológicas de proporcionar autenticidad e integridad. No obstante, en el corto plazo, mientras se formule este específico enfoque, debería asegurarse que un documento electrónico recibiera el mismo reconocimiento legal que un documento tradicional en papel acompañado por una firma manuscrita si el documento electrónico está acompañado por una firma digital y un certificado emitido por una unidad de certificación establecida y operando de acuerdo a los requisitos estándar.

Los documentos electrónicos "públicos" deberían entrar en una categoría especial, y quizás deberían ser reconocidos legalmente únicamente cuando estuvieran acompañados por una certificación emitida por una autoridad certificante licenciada. Aún cuando los escribanos públicos probablemente no recibirían con bienvenida esta perspectiva, uno podría preguntarse si las autoridades de certificación tienen un rol notarial para cumplir en el futuro digital y si las autoridades de certificación deberían tomar a su cargo muchos de los roles de los escribanos públicos en el mundo electrónico. Si esto es así, ¿cómo podríamos asegurar que los requerimientos de licencia no se usen para limitar la cantidad de autoridades de certificación y de esta manera restringir la competencia entre las autoridades certificantes?

4. Reglamentación de la Encriptación

Ahora nos volvemos hacia el otro gran tópico que reglamenta la Comunicación, denominado encriptación. En razón de que la encriptación ha sido un tema que provocó considerablemente más debate y comentario que las firmas digitales, nosotros comentaremos brevemente esta parte de la Comunicación.

Como la Comunicación reconoce correctamente, el desarrollo del comercio electrónico y de muchas otras aplicaciones de la sociedad de la información dependerá de la capacidad en términos de eficiencia y costo para mantener la confidencialidad de las comunicaciones electrónicas[18]. La Comunicación proporciona distintos ejemplos en los cuales este requerimiento de confidencialidad resulta particularmente claro, incluyendo telecompras y telebancos (donde los consumidores deben recibir la garantía acerca de qué datos personales -tales como los números de sus tarjetas de crédito- permanecerán confidenciales). Comunicaciones de negocios especialmente sensitivas tales como cotizaciones proyectadas, resultados de investigaciones y documentos similares (respecto de los cuales las compañías deben recibir protección contra el espionaje industrial) y aplicaciones telemáticas para la salud (donde los pacientes deberían ser protegidos contra la revelación no autorizada de sus archivos médicos). Como se ha hecho notar anteriormente en la sección introductoria de la tecnología, sistemas de encriptación simétricos resultan corrientemente la vía principal para obtener la confiabilidad de comunicaciones electrónicas. Tal como muchos lectores saben, ha tenido lugar un animado debate acerca de la reglamentación de la encriptación, y la Comisión tomó una posición clara y definida con respecto a los principales temas en este debate. En particular, la Comunicación contempla los siguientes temas:

- Medidas de control de exportaciones
- Medidas de control doméstico
- Sistemas de depósito y recuperación de claves
- Consideraciones relativas a la privacidad

⇨ Medidas de control de exportaciones

Como hace notar la Comunicación, han sido impuestos respecto de la encriptación, ciertos controles de exportación en un esfuerzo para privar a los opositores extranjeros de los beneficios de una sólida criptografía. Internacionalmente, tales controles se han impuesto bajo el así llamado Arreglo de Wassenaar[19], que reemplazó la lista COCOM. La exportación de ciertas tecnologías de exportación está controlada por la Unión Europea bajo la Regulación del Uso Dual de Diciembre de 1994[20]. Como lo señala la comunicación, en la medida en que las Regulaciones de Uso Dual permiten el control de despachos de productos de criptografía de productos de un Estado Miembro a otro, podían conducir a distorsiones en el funcionamiento del Mercado Unico.

Con respecto a las acciones de política a tomarse en el área de control de exportaciones, la Comunicación no sugiere ninguna acción relativa al arreglo de Wassenaar, probablemente porque la Comisión no desea ser vista como excediendo los límites de su autoridad en una materia sensitiva para la seguridad nacional. No obstante, la Comunicación afortunadamente sugiere que las reglamentaciones sobre el Uso Dual deberían

liberalizarse[21]. En particular, la Comunicación sugiere la progresiva eliminación de controles intra-comunitarios sobre productos comerciales de encriptación[22].

⇨ Medidas de control doméstico

En comparación con los controles de exportación sobre la encriptación, el control doméstico es, tal como la Comisión lo hace notar, relativamente infrecuente. Entre los Estados Miembros de la Unión Europea, solamente Francia tiene una regulación comprensiva acerca de criptografía. No obstante, se está produciendo actualmente un intenso debate en distintos países europeos (y también en los Estados Unidos de América) en lo que respecta a la posibilidad de adoptar ese tipo de legislación. Como indica la Comunicación, las autoridades nacionales de aplicación de la ley y las agencias nacionales de seguridad favorecen los controles domésticos sobre la encriptación en razón de que los mismos temen que el difundido uso de comunicaciones encriptadas disminuirá su posibilidad de luchar contra el crimen y prevenir el terrorismo.

La Comunicación hace notar que los propuestos mecanismos para el control doméstico podrían hacer que el uso de la encriptación (o por lo menos ciertas formas de encriptación) resultaran ilegales en tanto no hubieran sido autorizados. Alternativamente o adicionalmente, proveer e importar productos y servicios para la encriptación (o ciertos productos y servicios, tales como los que empleen fuertes técnicas de encriptación) deberían ser colocados bajo un esquema que requiriera autorización. El objetivo principal de estos regímenes es asegurar que la encriptación disponible para usuarios finales sea relativamente débil (o lo que es igual, prácticamente inútil) o se halle sujeta a una posibilidad de acceso por organismos gubernamentales por medio de un esquema de depósito de la clave u otros similares.

La Comunicación resulta refrescantemente sagáz en su juicio acerca de tales mecanismos domésticos de control. Básicamente, llama la atención acerca de que tales mecanismos podrían resultar inútiles y contraproducentes. Los mismos no impedirían a los criminales usar tecnologías efectivas de comunicación, pero "muy bien podrían impedir a las compañías y ciudadanos protectores de la ley protegerse a sí mismos contra ataques criminales"[23]. Más aún, este tipo de regulaciones al establecer diferentes reglas que gobernaran el uso y venta de productos para encriptación podrían crear obstáculos de funcionamiento del Mercado único y ésto proporciona una importante base constitucional para las iniciativas de la Comisión en esta área. Además, la formulación de leyes regulando la encriptación tendrá un directo efecto sobre la privacidad y sobre las libertades de palabra y asociación. Por todo ello, nosotros solamente podemos esperar que los Estados Miembros comprenderán la inteligencia del enfoque de la Comisión acerca de una regulación de la encriptación.

⇨ Sistemas de depósito y recuperación de claves

Los sistemas de depósito y recuperación de claves se encuentran entre los métodos que han sido sugeridos para controlar el uso de la encriptación en conexión con actividades ilegales. Bajo un sistema de depósito de claves, una copia de la clave relevante debería ser depositada sea en poder de una agencia oficial de aplicación de la ley o sea a una de las así llamadas terceras partes confiables, los que podrían ser requeridos para revelar la clave a agentes gubernamentales bajo ciertas circunstancias. Bajo un sistema de recuperación de clave se proporciona al gobierno o a la tercera parte confiable información acerca de la clave que debería permitir a las agencias de aplicación de la ley "recuperar" la clave si ello resulta necesario para revisar un mensaje con propósitos de investigación policial.

La Comunicación adopta una posición apropiadamente negativa respecto de sistemas de depósito y recuperación de claves. Tal como lo señala la Comisión[24], este tipo de sistemas resultarían inefectivos para propósitos de aplicación de la ley en la medida en que podrían ser fácilmente circunvalados. Al mismo tiempo, los sistemas de depósito y recuperación de claves disminuirían significativamente la atracción de la encriptación para los usuarios. Obviamente, cualquier forma en que una tercera parte se involucre en una comunicación confidencial incrementa la vulnerabilidad de la misma y en consecuencia, disminuye la confianza en la confidencialidad de la comunicación electrónica. Se presentan en conexión con todo esto serias preocupaciones con relación a la privacidad. Más aún, los sistemas de depósito y recuperación de la clave impondrían costos significativos para el uso de la encriptación, especialmente si tales sistemas debieran implementarse a una escala global. En resumen, las consecuencias adversas que derivarían de la imposición de sistemas de depósito o recuperación de las claves sin proporcionar ningún beneficio en términos de aplicación de la ley podrían conspirar contra el desarrollo del comercio electrónico.

⇨ Consideraciones relativas a la privacidad

Aún cuando reconociendo que consideraciones relativas a la seguridad nacional y a la aplicación de las leyes pueden en algunos casos prevalecer sobre los derechos a la privacidad, la Comunicación señala la importancia de la encriptación para el mantenimiento de la privacidad. En particular, mediante el empleo de métodos de encriptación los "controladores de datos" pueden cumplir sus obligaciones bajo el Derecho de la Comunidad Europea sobre Protección de los Datos, para proteger los datos personales.

Más puntualmente, la Comunicación subraya que la Comisión podría usar la Directiva de la Comunidad Europea sobre la Protección de los Datos y los poderes de la Comisión para aplicar las reglas de la Comunidad Europea

acerca del libre movimiento de bienes y servicios en orden a atacar determinadas legislaciones que reprimen el uso de la encriptación. Tal como la Comunicación hace notar, el libre flujo de los datos personales a lo largo de mercado Interno depende de la capacidad de los métodos de encriptación para "viajar" con la información personal que están asegurando. En consecuencia, dar lugar a que reglamentaciones de los Estados Miembros acerca de encriptación puedan obstaculizar el flujo de información causaría restricciones en el flujo de bienes y servicios entre los Estados Miembros. Tal como la Comunicación hace notar "cualquier regulación impidiendo el uso de bienes y servicios de encriptación a lo largo del mercado interno impediría en consecuencia el libre flujo de información personal y la provisión de bienes y servicios relacionados[25].

Orientaciones políticas de la Comisión

Al diseñar sus orientaciones políticas acerca de encriptación, la Comisión sin dejar de reconocer la competencia de los Estados Miembros con respecto a la seguridad nacional y la aplicación de las leyes indica que podría no hesitar en tomar acción contra regulaciones acerca de la encriptación que infrinjan el derecho de la Comunidad Europea, incluyendo la legislación de la Comunidad Europea acerca del libre movimiento de bienes y servicios y sobreprotección de los datos. A este respecto, la Comunicación hace notar que los Estados Miembros están obligados a notificar a la Comisión acerca de nuevas reglas nacionales que pudieran crear obstáculo al mercado interno e indicar que tales notificaciones deben proveer las bases para las acciones de la Comisión[26].

Debe ciertamente darse la bienvenida a esta orientación política. Indudablemente la Comisión está en lo cierto cuando afirma que no existirá un mercado interno para el comercio electrónico sin un mercado interno para la criptografía. Resulta por ello vital la armonización de las reglas de los Estados Miembros sobre la criptografía para evitar inconsistencias y la Comisión tiene un rol esencial que cumplir en esta tarea.

Además, la orientación internacional de la comunicación es importante. Como hace notar la Comunicación, la naturaleza global del comercio electrónico requerirá a la Comunidad Europea procurar un marco legal internacionalmente compatible para la firma digital y la encriptación, incluyendo el establecimiento de estándares técnicos internacionales (necesarios para la interoperabilidad) y reconocimiento mutuo de certificados sobre una base internacional. Nosotros podemos esperar que la Comisión promoverá su iluminada política de criptografía con sus más importantes socios comerciales, así como con las importantes organizaciones internacionales tales como la Organización Mundial del Comercio y la OECD.

En lo que a su programa futuro concierne, la Comisión intenta organizar una audiencia internacional con relación a los cuestiones que se tratan en la Comunicación durante el primer trimestre de 1998 y realizar una propuesta para posteriores acciones (quizás incluyendo una directiva acerca de firmas digitales) durante el segundo trimestre de 1998. Finalmente, y en forma apropiadamente ambiciosa, la Comunicación fija como un objetivo para el año 2000 como fecha para el establecimiento de un marco Europeo común respecto de criptografía.

5. Conclusión

Un viento refrescante está soplando desde Bruselas. Por primera vez desde que comenzó el debate sobre criptografía una Comunicación gubernamental ha reconocido claramente la necesidad del reconocimiento legal de las firmas digitales a una escala global y de una disponibilidad irrestricta por parte del público de técnicas fuertes de encriptación. Una pronta implementación de los objetivos políticos que subyacen a la Comunicación establecería alguna de las principales condiciones necesarias para el desarrollo del comercio electrónico y el amplio crecimiento de la Sociedad de la Información en Europa.

Notas

[1] COM (97) 503 (en adelante "Comunicación). Esta Comunicación fue precedida en abril de 1997 por la comunicación de la Comisión titulada "Una iniciativa europea sobre comercio electrónico". (COM (97) 157 final, 16.4.97). El DGXIII dio a conocer un Libro Verde sobre el mismo asunto el 24 de abril de 1994 titulado "Libro Verde sobre la seguridad de los sistemas de información", pero no se tomó ninguna acción posterior a esa época.

[2] Ver US Congress, Office of Technology Assessment Issue Update on Information Security and Privacy in Network Environments, Washington, DC, 1995, en 49.

[3] La capacidad para descubrir la clave privada a partir de la clave pública se incrementa en tanto que la tecnología (y la potencia de los computadores) progresa. En consecuencia, la longitud de la clave necesaria para obtener una firma digital confiable deberá estar bajo constante revisión, tal como lo deberá estar la seguridad contínua del algoritmo del caso. La tecnología debería asegurar también la seguridad de la red. El manejo de las claves debería tener lugar dentro de un ambiente seguro.

[4] En el pasado, muchas publicaciones usaron la expresión "tercera parte confiable" para cubrir tanto las autoridades de certificación y depósito de claves como los agentes de recuperación. No obstante, la Comunicación, de acuerdo con las Líneas de Guía de la OECD de Política de Criptografía (27 de marzo de 1997), usa las palabras "autoridad de certificación" para aquellas entidades que llevan a cabo servicios de integridad, en tanto que usa el término "terceras partes confiables" exclusivamente para aquellos organismos que desempeñan servicios relativos al acceso legítimo al acceso de

encriptación (depósito de claves y recuperación de claves).

[5] Usualmente el autorizante del certificado genera sus propias claves privada y pública que proporciona como parte de su solicitud a la autoridad certificante, pero es igualmente posible organizar un sistema en que las autoridades de certificación generen el par de claves.

[6] Por ejemplo, en Bélgica la compañía *Isabel* proporciona servicios de certificación con el sector bancario y la compañía *Belsign* provee tales servicios en una forma más amplia.

[7] Ver la Sección VI (Estructura de las Propuestas), parágrafo 43 del Documento de Consulta Pública acerca de propuestas detalladas para Legislación "Licensing of Trusted Third Parties for the Provision of Encryption Services"(UK Department of Trade & Industry, Marzo 1997). Aún cuando la ley alemana de firmas digitales establece un sistema de licencias para las autoridades de certificación (ver §4 de la Ley de Firma Digital), este sistema no parece ser obligatorio. **N. del T.:** La Ley de Firma Digital Alemana se publicó en DAT, No. 106, pág. 19.

[8] Ver (A/CN,9/437).A/CN,9/WG.IV/WP.71, y A/CN.9/WG.IV/WP.73). **N. del T.:** Texto castellano publicado en págs. 23/27 de este número.

[9] En la discusión legislativa acerca de la discusión de la Ley de Firma Digital, se decidió, en razón de la novedad del tema, no incluir disposiciones especiales acerca de responsabilidad pero analizar en el futuro si resultarían apropiadas reglas especiales de responsabilidad.

[10] Ver la Sección VI (Estructura de las Propuestas) Parágrafo 43 del Documento de Consulta Pública acerca de Propuestas Detalladas para Legislación *"Licensing of Trusted Third Parties for the Provision of Encryption Services"*(UK Department of Trade & Industry, Marzo 1997.

[11] Wright, B., *Eggs in baskets*: distributing the risks of electronic signatures, *The John Marshall Journal of Computer & Information Law*, Vol. XV, No. 2: 189-201 (1997).

[12] Ver Lamberiere, I., *La valeur probatoire des documents informatiques dans les pays de la CEE, Revue Internationale de Droit Comparé*, No. 3 (1992).

[13] Por ejemplo, el Artículo 1341 tanto del Código Civil Belga como del Código Civil Francés, requieren evidencia escrita cuando el valor del contrato (por ejemplo un contrato de ventas) excede ciertos límites.

[14] Por ejemplo en Alemania. Para mayores comentarios sobre este tema en particular ver Blechschmidt, R., *The German Basic Electronic Data Interchange Model Agreement Versus the European Model EDI Agreement: Some Reflections on German Law, The EDI Law Review*, No. 3, 1996, en 107-124

[15] Comunicación Sección IV.1.2 (ii)

[16] Para UNCITRAL ver las Recomendaciones de 1995 (A/40/17),Ley Modelo de UNCITRAL para el Comercio Electrónico del 14 de junio de 1996 (A/51/17). Para TEDIS, ver TEDIS Situación Jurídica de los Estados Miembros respecto de las transferencia de datos, Bruselas, comisión de las Comunidades. Para el Grupo de Trabajo para la Facilitación del Comercio UN/ECE ver Recomendaciones UN/EC No. 12; UN/E No. 13; UN/EC No. 14.

[17] Un similar enfoque funcional se incorpora al Artículo 7 de la ley Modelo UNCITRAL para Comercio Electrónico.

[18] Comunicación, Sección III.1 (iii).

[19] Acuerdo de Wassenaar sobre controles de exportación para armas convencionales y bienes y tecnologías de uso dual (Diciembre 19, 1995). Http://www2.nttca.com:8010/informofa/press/c_s/wassenaar.html; http://ideath.parrhesia.com/wassenaar/wassenaar.html

[20] Consejo de Regulación (EC) 3381/94, 19.12.94. Consejo de Decisión 94/942/CFSP, 19.12.94, OJ L 367/8 (31.12.94), establece la lista de los bienes de uso dual cubierto por la Regulación.

[21] Comunicación, Sección IV.2(ii)

[22] Id.

[23] Comunicación, Sección III.2.1.

[24] Comunicación, Sección III.2.3.

[25] Comunicación, Sección III.2.4. Ver también Comunicación, Sección III.3 (v).

[26] A este respecto, debe hacerse notar que el gobierno de Francia ha notificado a la Comisión acerca de sus propuestas legislativas pendientes acerca de encriptación.

Abstract

A comment about the recent Communication of the European Commission entitled "Ensuring Security and Trust in Electronic Communication: Towards a European Framework for Digital Signatures and Encryption" which deals with a European framework of certification authorities and the encryption systems legal regime. The article provides an introduction to the relevant technology and a description and analysis of the Communication.

Voces

Autoridad - Certificación - Clave - Comisión - Comunicación Criptografía - Depósito - Digital - Encriptación - Exportación Firma - Europa.

Rosa Julià Barceló es una investigadora en el Centre de Recherches Informatique et Droit de la Faculté Universitaire Notre Dame de la Paix, en Namur (Bélgica).

Thomas Vinje, abogado, socio en la oficina de Bruselas de la firma Morrison & forster LLP.